National Security Agency

Managers' Internal Control (MIC) Program

Vulnerability Assessments

DoD FY06 MIC Program Conference

Bob Crouse, CPA

NSA's MIC Program

Brief History:

- Essentially a paper process
- October 2002 – New Comptroller hired
- January 2003 – Organization established to assume administration of MIC Program
- December 2003 – Hired contractor to assist in enhancing the MIC Program

NSA's MIC Program

FY03 Goal – Incremental Improvement:

- Heighten awareness through IC training
- Emphasize honest vulnerability (self) assessments
- Ensure compliance w/DoD reporting guidelines

NSA's MIC Program

FY04-05 Focus –Improve the Assessment Process:

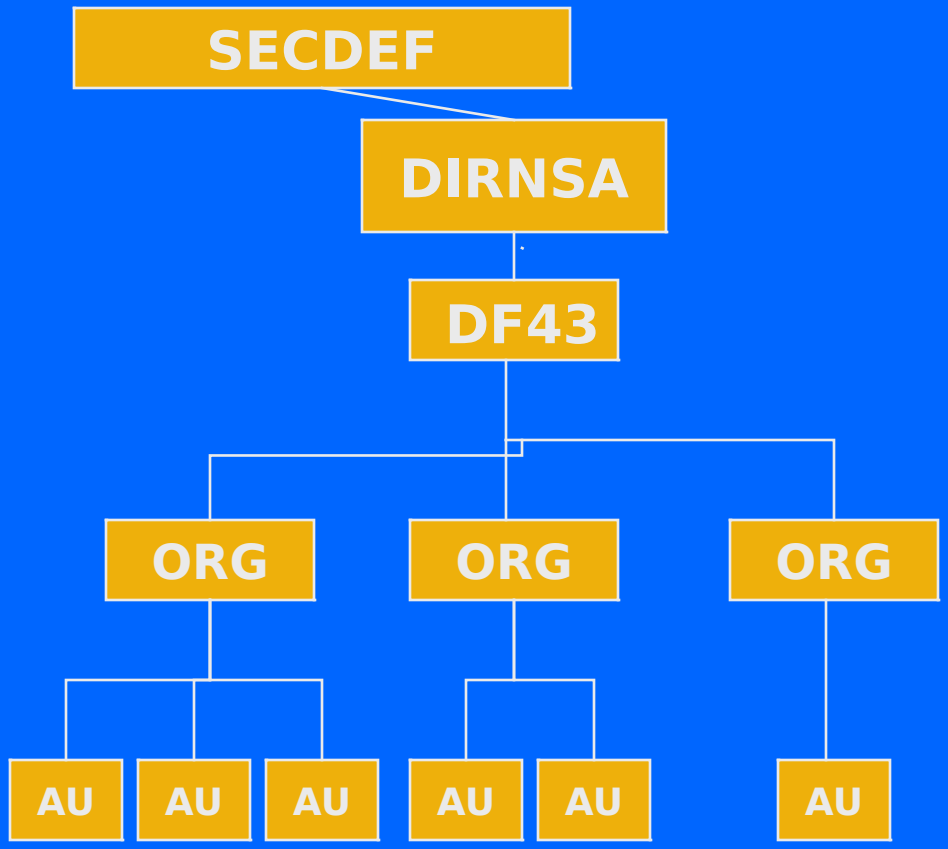
- **Emphasize accountability**
- **Incorporate GAO control standards**
- **Incorporate NSA OIG Challenges**
- **Incorporate DoD Systemic Weaknesses**
- **Require explanations and specific examples**
- **Address validation (tests) of controls**
- **Submit VAs to DF43 at Alpha+2 level**
- **Improve support for DIRNSA's SoA**

Key Deliverables

Each Directorate and Field Site (approx. 60 “reporting entities”) required to submit:

1. A Statement of Assurance (SoA) including:
   - Cover letter
   - Tab A
   - Tab B (if applicable)
2. Vulnerability assessments (VA) for each assessable unit of the organization

The VA process flow…



MIC Program Timeline

- January – April: Revise IC Program and develop training
- May – June: Provide NCS training (RESM-2455) to MC Coordinators, Evaluators, Approving Officials, etc.
- August 1: Orgs submit SoAs and VAs to DF43
- August: DF43 review SoAs and VAs, provide assistance to orgs, prepare DIRNSA's SoA
- September 1: Submit DIRNSA's SoA to SECDEF

The Vulnerability Assessment (VA)

…is not an extensive or in-depth analysis.

…is a limited review mechanism for determining your organization's susceptibility to fraud, waste or abuse of resources and the potential for not achieving the objectives of management control.

Basis for management's assertion

The vulnerability assessment(s) should provide the basis for management's assertion (SoA) regarding the existence and effectiveness of controls within the organization.

Vulnerability Assessment Form

Page 1

Before getting started…

- Define terms
  - Assessable Unit (AU)
  - Mission
  - Risk/Vulnerability
- Understand your responsibility as
  - Evaluator
  - Approving Official

Before getting started…

- Understand key issues
  - NSA Management Challenges
  - NSA OIG Challenges
  - DoD Systemic Weaknesses

Defining the "Assessable Unit"

An assessable unit

…should be a subdivision of an organization that ensures a reasonable level of span of IC to allow for adequate control analysis._

Management defines the appropriate number/level of Assessable Units (AU) and completes a Vulnerability Assessment (VA) for each AU.

Defining your mission

- **What do you do?**

- **Efforts should tie into your organization's**
  - **Strategic Plan**
  - **Goals and Objectives**
  - **Budget**

Assessing your risks/vulnerabilities

Risk is the probability (likelihood) that an event or action may adversely affect (impact) the organization.

Risk considerations…

Management should evaluate risk in terms of:

1. **Consequence**
2. **Likelihood of occurrence**
3. **Cause**
4. **Cost/benefit of lowering risk**

Guide for Evaluating Risk

Likelihood \ Consequence	Low	High
High	II Area of minimal concern	**IV** **Area of most concern**
Low	I Area of least concern	III Area of moderate concern

Your role in the VA process…

The *Evaluator* and *Approving Official* should have sufficient knowledge of the organization and internal controls to identify the key processes, risks and vulnerabilities of their organization.

Note: *VA should only be signed by NSA Civilian Employee or Military Personnel.*

NSA Management & OIG Challenges

- Information Sharing (OIG)
- Developing a "Need to Share" Culture (MC)
- Denial & Deception (OIG)
- Analysis Driven, Service Based Ops (MC)
- Integrating Computer Network Ops (MC)
- Mission Assurance (OIG)
- SID/IAD Relationship (MC)
- Exploitation of Digital Communications (OIG)
- System Engineering (OIG)
- Information Assurance for DoD Systems (OIG)

NSA Management & OIG Challenges

- Polygraph Backlog (OIG)
- Managing the "Revolving Door Syndrome" (MC)
- Recruitment & Retention of Linguists (OIG)
- Improve the Cache of Leadership at NSA/CSS (MC)
- Building the Bench (MC)
- Field Governance (OIG)
- Certification and Accreditation of Networks and Systems (OIG)
- Security for National Security Systems & Critical Infrastructures (OIG)
- Acquisition Management (OIG)
- Financial Management (OIG)

DoD Systemic Weaknesses

- DoD Financial Management Systems and Processes
- Management of Information Technology and Assurance
- Environmental Liabilities
- Personnel Security Investigations Program
- Real Property Infrastructure
- Government Card Program Management
- Valuation of Plant, Property and Equipment on Financial Reports
- Valuation of Inventory of Financial Reports
- Improper use of Non-DoD Contracting Vehicles

What controls are in place?

Given your organization's risks and vulnerabilities, what do you do to prevent or detect such threats and how do you minimize their impact if/when they occur?

Consider GAO "control activities" (policies & procedures, approval, authorization, reconciliation, documentation, security, etc.)

How/When were controls last tested?

Often times, management assumes controls are in place, but for various reasons (e.g., reorganization, employee turnover) they are not.

How is tests of controls (monitoring) performed and documented and when was it done most recently?

Are controls adequate?

After identifying your “high” risk vulnerabilities and the extent to which internal controls are operating, does your organization need additional controls?

Consider cost v. benefit & tolerable risk.

Vulnerability Assessment Form

Page 2

GAO Standards for Internal Control

Be conscious of…

- Linkage within the VA:
  - Risks identified
  - Controls identified for mitigating risks
  - Tests of controls
- Linkage between information included in the VA and that communicated in the SoA.

Final thoughts…

- Keep it simple
  - Terminology can be a barrier
  - Translate into operations language
  - Capitalize on what's already being done
- Major marketing effort
  - Achieving buy-in is not easy
    - Organization culture
    - Mission v. administrative burden
    - "This is a Finance issue"
  - Must hit home
- Training, training, training!